Blockchain Security Alliance

BEOSIN Blockchain Security × BUIDLER DAO × LegalDAO × Footprint Analytics

Global Web3 Security Report 2022

& Crypto Regulatory Compliance Research

SECURING
BLOCKCHAIN ECOSYSTEM

BEOSIN

CONTENTS

Preface

As the blockchain industry ushers in a new period of development in 2022, various security risks are also emerging. The high occurrence of blockchain security incidents that emerge one after another has been a serious challenge to the blockchain industry.

From Beosin's statistics in 2022, multiple projects have been hacked and the huge economic losses have seriously affected the security and stability of the blockchain ecosystem.

In terms of regulation and compliance, there is still a long way to go to improve and establish the relevant system of blockchain industry, and the intervention of relevant departments and effective promotion of industry practitioners are urgently needed. The current development trend of the blockchain industry is generally positive and the future development potential is promising, but it is also important to recognize that the chaotic security situation and multi-faceted security challenges urgently require the strengthening of blockchain security regulation and compliance.

In this 'Global Web3 Security Report 2022 & Crypto Regulatory Compliance Research', we will recap on the top 10 security incidents and analyze the global Web3 security statistics from multiple dimensions in section one. The second section will introduce global crypto crime statistics, major financial events, and regulatory compliance in different countries or regions. In section three, security guidelines and solutions will be provided for web3 users. The final section is Beosin's 2023 outlook on the blockchain security industry.

I.

2022 Global Web3 Security Statistics

Contributors:
Beosin research team – Mario, Donny

Data source (As of Dec 20, 2022):
https://www.footprint.network/@Beosin/Footprint-Beosin-2022-Report

In 2022, Beosin EagleEye monitored over 167 major attacks in the Web3 space, with a total loss of approximately $3.6 billion from all types of attacks, an increase of 47.4% from 2021. Of these, 10 security incidents lost over $100 million in a single attack and losses of 21 security incidents ranged from $10 million to $100 million.

$2,444,195,869
2021 Total Loss

$3,603,840,802
2022 Total Loss

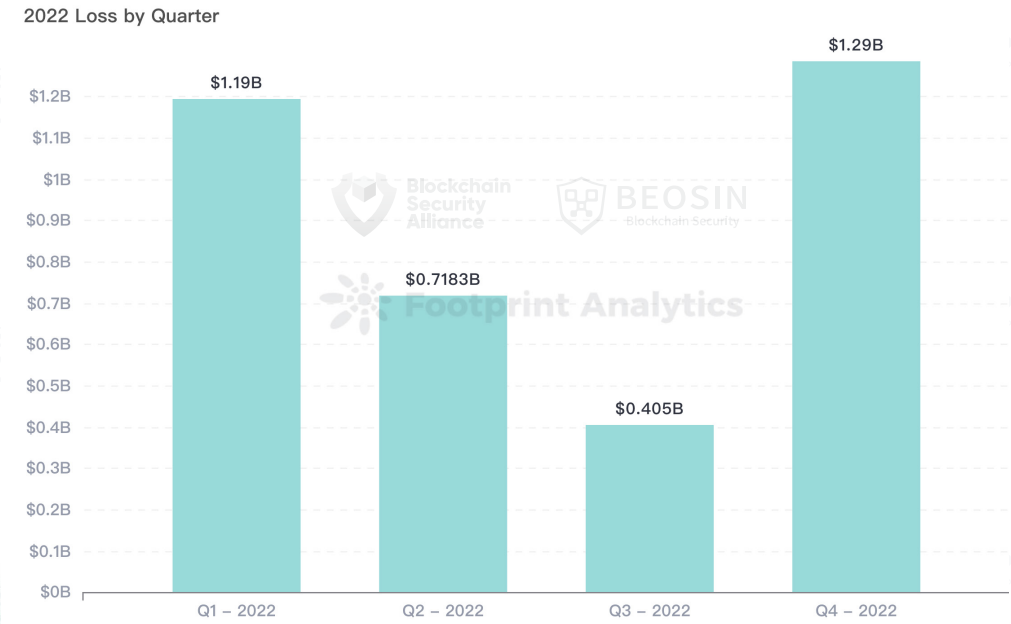
By project type, the 12 cross-chain bridge incidents have caused a total loss of approximately $1.89 billion, ranking first among all project types. DeFi-type protocols were attacked 113 times, or about 67.6% of the total attacks, making it the most frequently attacked project type.

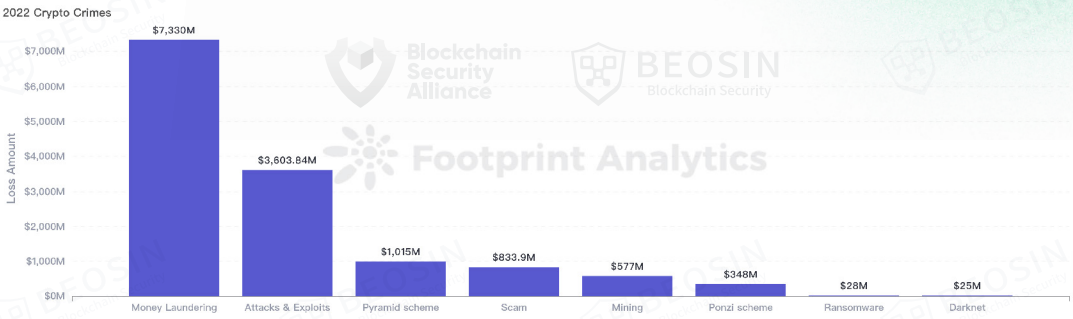
A total of 20 public blockchains had major security incidents in 2022, with the top three by amount lost being Ethereum, BNB Chain, and Solana; and the top three by number of attacks being BNB Chain, Ethereum, and Solana.

Vulnerability exploits ranked highest in both frequency and loss throughout the year, with $1.458 billion lost in 87 vulnerability exploits.

Of the 167 major attacks monitored in 2022, audited and unaudited protocols accounted for roughly 50/50, at 51.5% and 48.5% respectively.

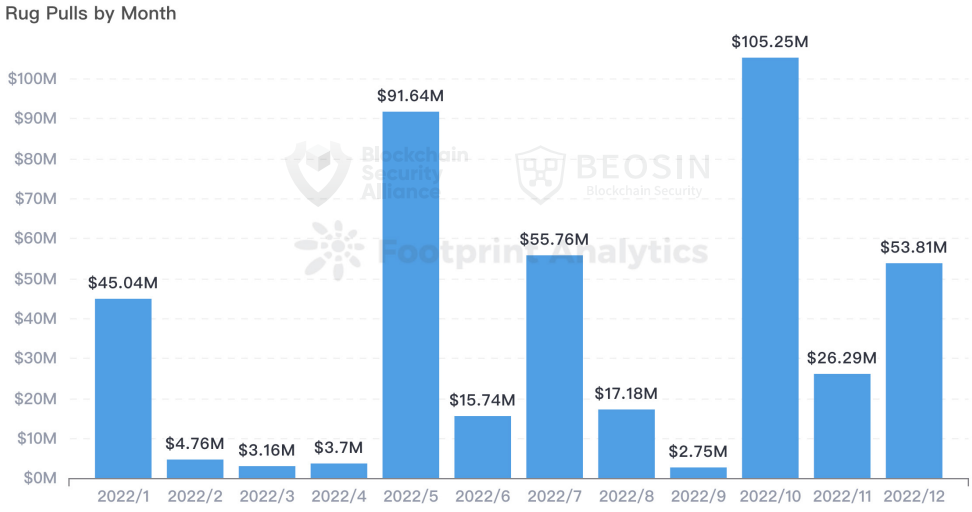
Approximately $1,396 million of stolen funds were deposited into Tornado Cash in 2022, representing 38.7% of the funds lost in all attacks. Only 8% of the stolen funds were recovered for the year, or around $289 million.





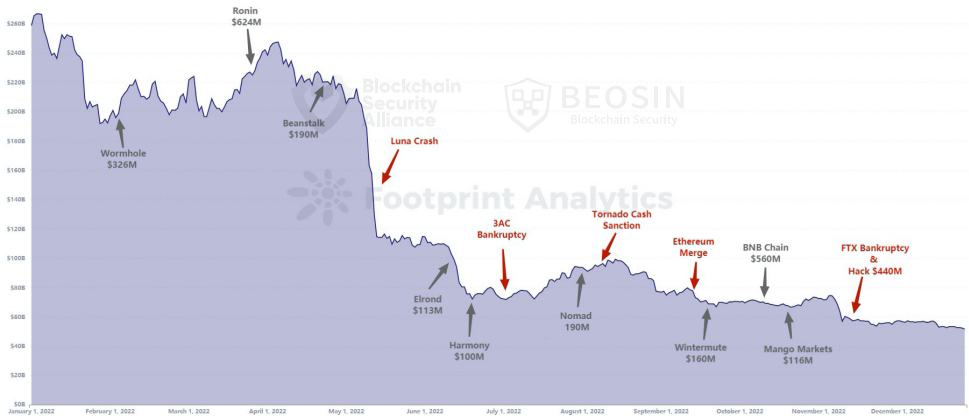
Global crypto crimes amounted to $13.76 billion for the year 2022 (financial crimes are excluded), with money laundering accounting for $7.33 billion, attacks/exploits $3.6 billion, pyramid schemes $1 billion and scams $830 million.

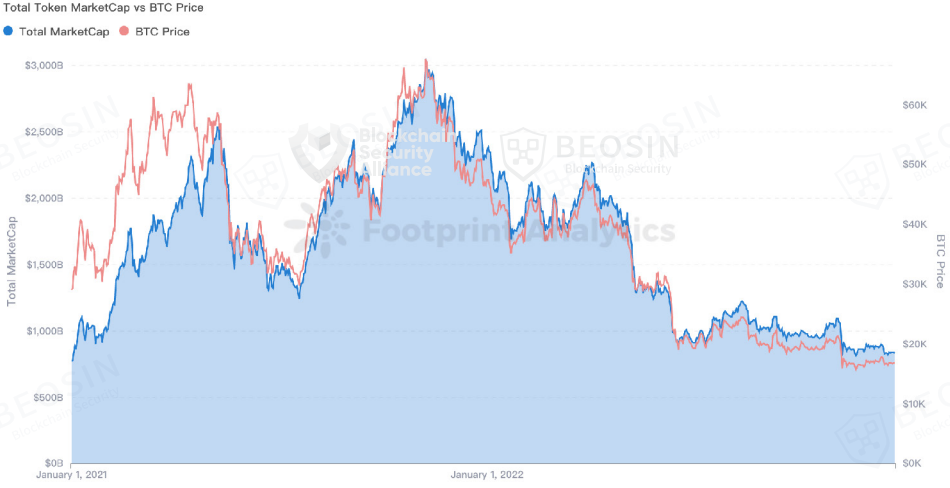
Among the scams in 2022, 243 Rug pulls have involved a total amount of $425 million (excluding the $440 million FTX event). Approximately 86.4% of the project rugged with funds in the range of $1k – $1M.



Global TVL shrank significantly in 2022, ending the year with TVL down approximately 80% from its peak at the beginning of the year. The market was heavily impacted by a series of black swan events represented by Three Arrows Capital, Terra Luna and FTX.

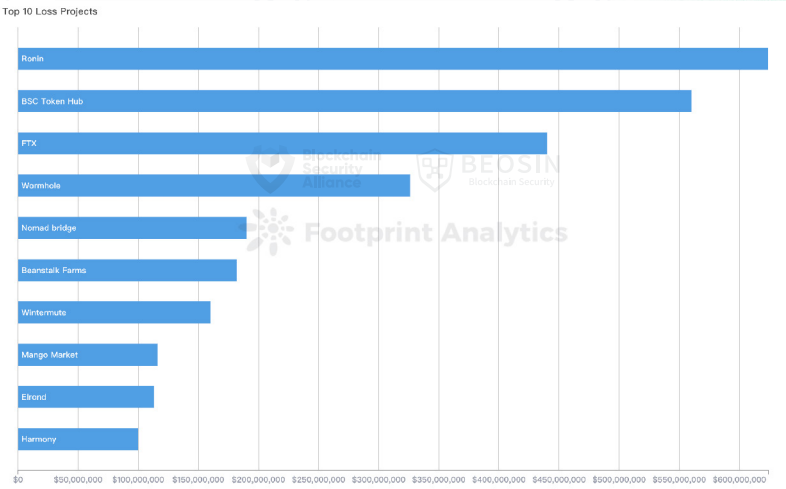
2022 TVL Trend





Despite a significant shrinkage in global crypto marketcap, the overall crime figure for blockchain in 2022 still reached $13.7 billion, with a significant increase in attacks compared to 2021. The past 2022 was a tough year for global blockchain security in general, and will place higher and more urgent demands on the security industry in 2023. Combating rampant hacking, accelerating the establishment of a global regulatory system, and bringing about technological breakthroughs to address existing industry shortcomings – these will be the key issues to be considered and urgently addressed in 2023.

1. Top Ten Security Incidents in 2022



No1. Ronin Network

Loss：$624 Million Attack Type：Social engineering

On 29 March 2022, the Axie Infinity sidechain Ronin was attacked and approximately $624 million in cryptocurrency was stolen. The hackers used the stolen private key to forge a withdrawal credential, which required at least five validators, and eventually the attackers managed to take control of five validators to steal the funds.

According to the investigation, the hackers sent a fake offer letter to Sky Mavis' engineers by way of social engineering, and the document allowed the hackers to compromise Ronin's system. After the attack, the stolen assets were sent to multiple addresses and laundered in batches through Tornado Cash. On 20 May, the Ronin attackers transferred the last batch of funds to Tornado Cash and all assets were laundered. On 28 June, Ronin announced its reopening on Twitter.

Beosin security team gave the following recommendations for such cross-chain bridge projects:1. Pay attention to the security of validator; 2. When the signature service is taken offline in the relevant business, the policy should be updated in time to close the corresponding service module, and the corresponding signature address can be discarded; 3. In multi-sig-nature verification, the multi-signature service should be logically isolated from each other, and the signature content should be verified independently; 4. The project owner should monitor the abnormal situation of funds in real time.

No2. BSC Token Hub (BNB Chain)

Loss: $560 Million Attack Type: Blockchain vulnerability

On 7 October 2022, BNB Chain's cross-chain bridge Token Hub was hacked. The hacker first paid 100 BNB to register as a Relayer by calling the contract at block height 21955968, and then acquired a total of 2 million BNB from BNB Chain's TokenHub contract. The hacker then pledged 900,000 of these BNBs on BNB Chain's lending protocol Venus and borrowed out 62.5 million in BUSD, 50 million in USDT, and 35 million in USDC.
Beosin security team found that due to the BSC Token Hub used a special pre-compiled contract for validating the IAVL tree when performing cross-chain transaction verification. The implementation is vulnerable, allowing an attacker to forge arbitrary messages.

On 24 October, Binance founder Changpeng Zhao said that the scope of the attacker's identity had been narrowed down with the help of law enforcement. In addition, CZ said Binance was able to freeze about 80 to 90 percent of the stolen funds, with actual losses in the range of $100 million.

No3. FTX: Hack or rug pull?

Loss: $440 Million Attack Type: Suspected rugpull

On 15 November 2022, shortly after FTX declared bankruptcy, FTX was announced that it had been hacked. Approximately $440 million was stolen. The administrator sent a message to the official telegram group stating that the bankrupt platform had been hacked and that all applications were malware. The administrator advised users to delete the app and not to visit the site or open their apps, as this would likely contain a Trojan horse. There are still many unknowns, many believe that this is likely to be an insider operation.

No4. Wormhole

Loss: $326 Million Attack Type: Contract vulnerability – validation issue

On 3 February 2022, Wormhole was hacked, resulting in a loss of approximately $326 million. Analysis by the Beosin security team found that the hackers had exploited a signature verification vulnerability in Wormhole contracts that allowed hackers to forge sysvar accounts in order to mint wETH. The vulnerability had been patched in Solana 1.9.4 and was still subject to a review process before it was finally live, and the hackers took advantage of this gap to attack contracts still using Solana 1.8 contracts.

Following the attack, Wormhole announced that it had restored its cross-chain bridge funding and was back online. Crypto investment fund Jump Crypto announced on 4 February that it had invested 120,000 Ether to cover the loss of the incident in order to support Wormhole's continued growth.

No5. Nomad bridge

Loss: $190 Million Attack Type: Contract vulnerability – validation issue

On 2 August 2022, Nomad, a cross-chain bridge protocol, was subjected to a massive hack that involved over 500 hacker addresses and caused a loss of $190 million. Beosin security team analysed the transaction and found that the project owner had incorrectly added 0x000...000 as an acceptable root, causing the judgement to hold, thus allowing the attacker to withdraw the funds in the contract.

As a result, any attacker could simply copy the first hacked transaction and replace it with an unused attack address, then click to send it through Etherscan to steal the funds. Also, since it was the Replica contract that was vulnerable, all its corresponding BridgeRouter-related DApps were affected, so the stolen funds exhibited a multi-token nature.

On August 3, Nomad released a note to call on whitehat hackers to return the stolen funds. As of August 15, the project has recovered $37 million.

No6. Beanstalk

Loss: $182 Million Attack Type: Flashloan

On April 17, 2022, the algorithmic stablecoin project Beanstalk Farms suffered a flashloan attack, with the protocol losing $182 million and the attackers making a profit of $80 million. The attackers transferred the entire $80 million to Tornado Cash soon after the attack.

The attackers initiated a proposal one day before the attack, which will withdraw the funds from the Beanstalk Protocol contract. The hacker gained a large reserve of funds via flashloan, which was then swapped repeatedly. A final vote on the proposal resulted in its being passed. In response to this incident, the Beosin security team recommends that: 1. the funds used for voting should be locked in the contract for a certain period of time and avoid using the current fund balance of the account to count the number of votes; 2. the project owner and the community should pay attention to all proposals and, if a malicious proposal occurs, it is recommended to discard the proposal; 3. Consider banning contract addresses from voting.

No7. Wintermute

Loss: $160 Million Attack Type: Private key compromise

On September 20, 2022, Wintermute lost $160 million in the DeFi hack. Analysis by Beosin security team found that the attackers frequently exploited 0x0000000fe6a... address to call the 0x178979ae function of the 0x00000000ae34...contract to transfer money to the attacker's contract. By decompiling the contract, it was found that calling the 0x178979ae function required permission checks, and by querying the function, it was confirmed that the 0x0000000fe6a address had setCommonAdmin permissions, and that the address had normal interaction with the contract before the attack, so it could be confirmed that the 0x0000000fe6a's private key was compromised.

On 21 September, Wintermute confirmed that it had used Profanity and an internal tool to create wallet addresses in June, and that the Profanity tool was at risk of private key bursting.

No8. Mango markets

Loss: $116 Million Attack Type: Price manipulation

On October 12, 2022, the Mango protocol on Solana was hacked, approximately $116 million was lost. The hackers used two accounts and a total of 10 million USDT as starting funds to leverage 100+ million of assets. The main reason for this attack was the leveraged contract did not limit the positions that Mango could open, allowing the attackers to raise the price of Mango tokens for profit.

No9. Elrond

Loss: $113 Million Attack Type: VM issue

On June 5, 2022, the blockchain network Elrond was hacked, with hackers "obtaining" nearly 1.65 million in EGLDs and dumping through the decentralised exchange Maiar, causing $EGLDs to plummet by 92%.

Elrond has posted a post-mortem that the attackers did not exploit any smart contract code vulnerabilities and that the problem was with the virtual machine. Previous bugs have been resolved and almost all of the stolen funds have been recovered. Any remaining missing funds from known bugs will be fully covered by the Elrond Foundation.

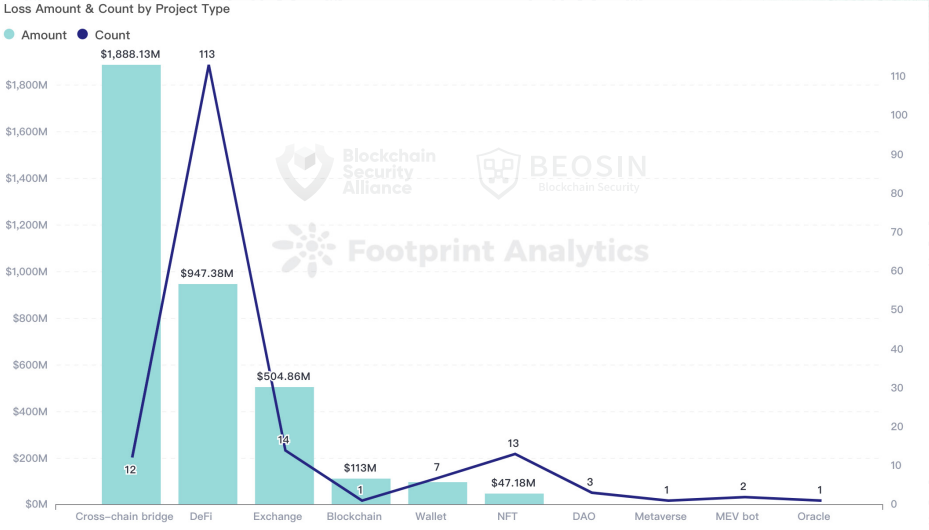
No10. Harmony

Loss: $100 Million Attack Type: Private key compromise

On June 24, 2022, the Harmony cross-chain bridge was attacked, costing approximately $100 million. Harmony's founder stated that the attack on Horizon was not due to a smart contract vulnerability, but rather to a private key compromise. Although Harmony stored its private keys encrypted, the attackers decrypted some of them and signed some unauthorized transactions.

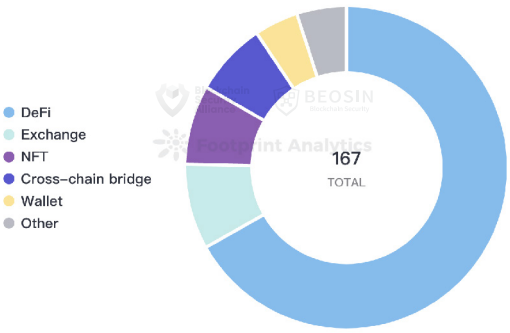
Immediately after the attack, Harmony stopped the Horizon Bridge to prevent further transactions. It then contacted the FBI and multiple partners to investigate. The hackers nevertheless laundered the stolen funds through Tornado Cash. On 27 July, Harmony issued a compensation proposal.

2. Types of Attacked Project



In 2022, 12 cross-chain bridge security incidents caused a total loss of approximately $1.89 billion, the highest loss of any project type. Five cross-chain bridge projects lost over $100 million in a single incident: Ronin ($624 million), BSC Token Hub ($560 million), Wormhole ($326 million), Nomad ($190 million) and Harmony ($100 million). The attack types mainly included social engineering, private key compromise, and blockchain/contract vulnerabilities, etc.

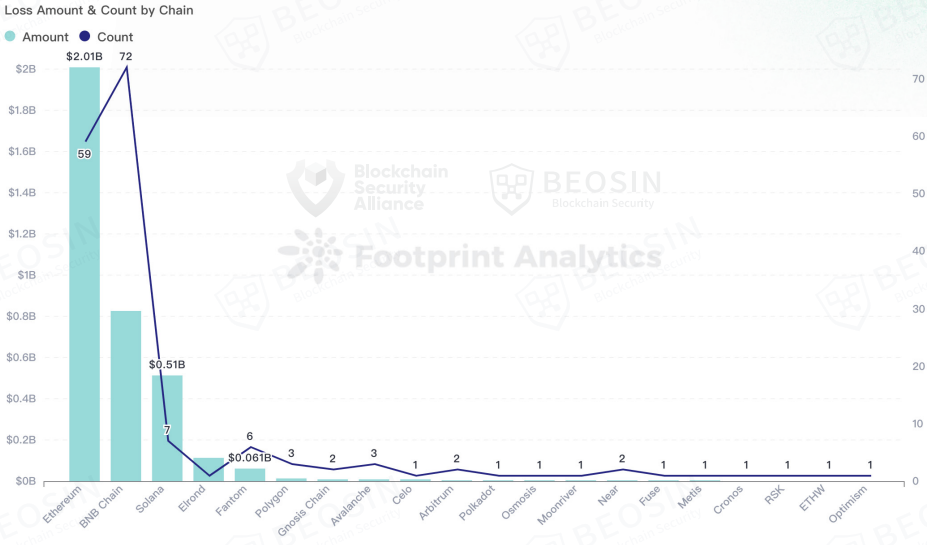
Market Share of Count by Project Type



Of the 167 major attacks for the year, DeFi-type projects were attacked 113 times, or approximately 67.6%, which is the most frequent type being attacked. DeFi ranks second in terms of losses after the cross-chain bridge, with a total loss amounting to approximately $950 million.

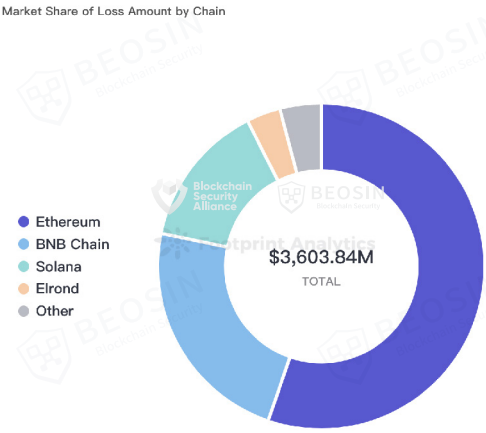
A total of 21 exchange and wallet security incidents throughout the year, resulting in a total loss of approximately $600 million. These incidents involved high amounts of money and a wide range of users, and their attack techniques were mainly private key compromises, contract vulnerabilities and supply chain attacks.

3. Loss by Chain



A total of 20 public chains have experienced major security incidents in 2022, with the top three by amount lost being Ethereum, BNB Chain, and Solana; and the top three by number of attacks being BNB Chain, Ethereum, and Solana.

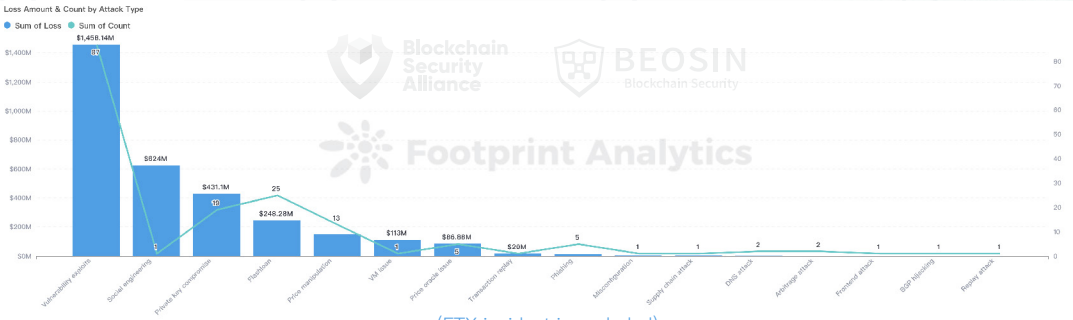
The 59 attacks on Ethereum caused $2.01 billion in losses, accounting for 55.8% of the total losses for the year.



There were 72 attacks on BNB Chain, with 70% of the loss in a range from one thousand to one million. Notably, approximately 64% of the projects attacked on BNB Chain were unaudited, and 80% of the unaudited projects were attacked by contract vulnerability exploits.

The seven attacks on Solana resulted in a total loss of $512.76 million, the highest average loss per incident across all chains.Major security incidents on the Solana chain include the Wormhole incident in February ($326 million), the Cashio incident in March ($48 million) and the Mango Market incident in October ($116 million).

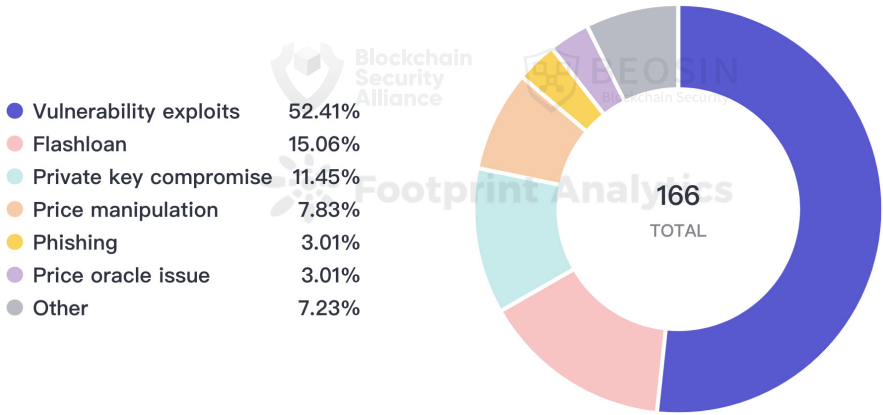
4. Attack Type



(FTX incident is excluded)

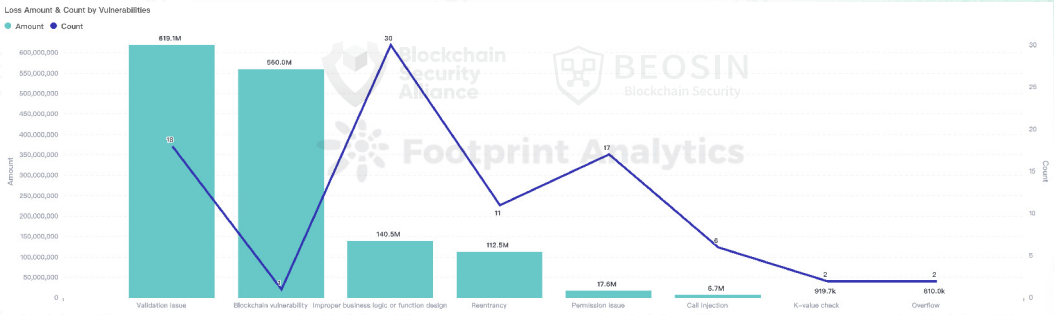
Vulnerability exploits saw the highest frequency and loss amount throughout the year. For the year 2022, $1,458 million was lost from vulnerability exploits in 87 attacks.

Market Share of Count by Type



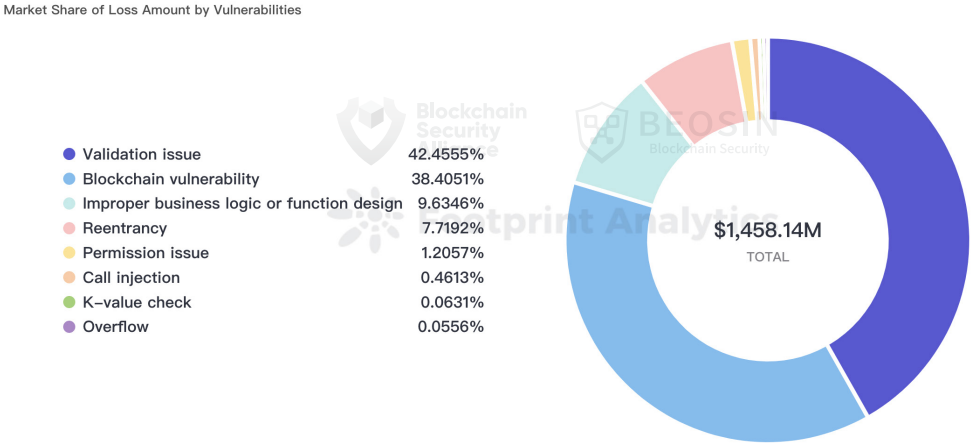
The second highest loss was caused by social engineering, which is the Ronin incident in March, resulting in $624 million in losses.

The third loss was from private key compromise, with 19 compromises resulting in a total loss of approximately $430 million, including eight incidents with a single loss of over $10 million. According to the findings of some incidents, the theft of private keys by team members/ex-members is frequent, which requires project owners pay extra attention to operational security and strengthen team management. There were also some cases of private key compromises due to the use of third-party tools, and projects are advised to conduct careful security assessments before using third-party tools.



A breakdown by type of vulnerabilities shows that the top three causes of loss were validation issues, blockchain vulnerability (BNB Chain incident) and improper business logic/function design and reentrancy.

Eighteen validation issues caused $619 million in losses, with major incidents including a signature validation vulnerability in the Wormhole incident and a message validation bypass issue in the Nomad bridge incident.



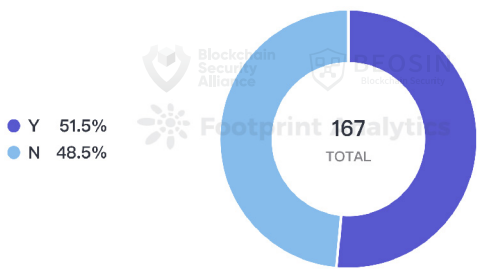
The most frequent issue was improper business logic/function design, with 30 occurrences. During Beosin's daily audits, this type of vulnerability is also the one that appears most frequently and is most likely to be overlooked by developers.

5. Audit Analysis

Of the 167 major attacks monitored in 2022, audited and unaudited projects account for almost half of the total, at 51.5% and 48.5% respectively.

Of the 86 audited projects, 39 attacks (45%) still originated from vulnerability exploitation. The quality the overall audit market is not promising. A review of these incidents by Beosin found that the vast majority of vulnerabilities were detect–able and fixable during the audit phase.

Whether Audited – Count



No projects that were attacked due to contract vulnerabilities in 2022 were audited by Beosin. It is recommended that projects must be audited by a professional security company before they go live in order to effectively safeguard assets.

6. Stolen Fund Flow

Approximately $1,396 million of stolen funds were transferred to Tornado Cash in 2022, representing 38.7% of all funds lost in attacks. Since Tornado Cash was sanctioned by the US OFAC in August, funds transferred to Tornado Cash have fallen significantly from the first half of the year. Only $44.85 million in stolen funds was transferred to Tornado Cash in the fourth quarter.

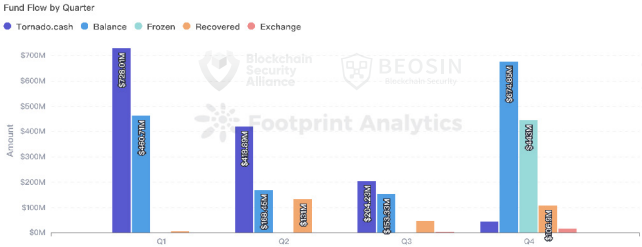
In 2022, approximately $289 million of stolen funds were recovered, represent–ing only 8% of all losses. The vast majority of this came from unsolicited returns from whitehat hackers.

Around $18.2 million of the stolen funds went to various exchanges. Often hackers who involve smaller amount of stolen funds would have transferred assets to exchanges immediately after the attack. It is particularly important for exchanges to be able to identify the hacker's address in time to block the transaction.

Fund Flow – table

Fund Flow	Sum of Amount
Balance	$1,457,339,412
Tornado.cash	$1,395,993,920
Frozen	$443,000,000
Recovered	$289,259,435
Exchange	$18,248,035

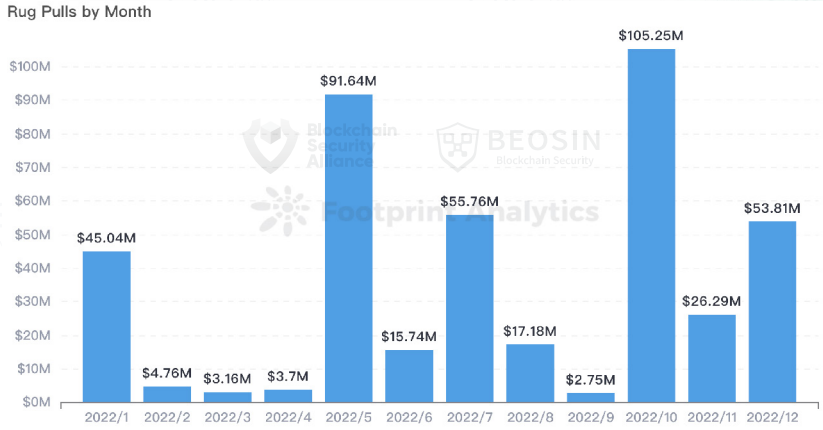
【All amounts are converted at the event time】



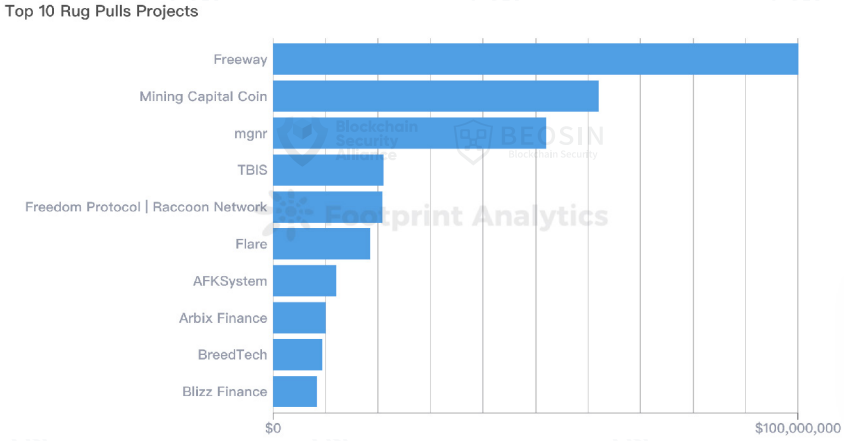
Approximately $443 million in stolen funds were frozen by exchanges, with the bulk of this amount stemming from the BNB Chain incident in October, when Binance immediately froze 80 to 90 percent of the hackers' funds, resulting in an actual loss of around $100 million for that incident.

7. Rug Pulls in 2022

There were 243 rug pulls throughout 2022, involving a total amount of $425 million (excluding FTX incident).



Of the 243 rug pulls, a total of 8 projects have rugged for $10 million or more, while 210 projects (approximately 86.4%) rugged with amounts between $1K – $1M.



In 2022, Rug pull events were characterised by the following features.

1. A high number of rugged projects throughout the year. On average, one project rugged every 1.5 days.

2. Short rug period. Most projects rugged within 3 months after going live, that's why most funding amount were in the range between $1K – $1M.

3. Most projects are unaudited. Some projects have hidden backdoor functions in their code, making it difficult for the average investors to assess the security of the project.

4. Social media information is lacking. At least half of the rug pull projects do not have a well-developed website, Twitter account, or Telegraph/Discord group.

5. Projects are not standardised. Some projects have official websites and whitepapers, but on closer inspection there are many spelling and grammatical errors, and some are even plagiarised in large sections.

6. The number of tokens launched under trending events has increased. Various kinds of tokens have rugged this year, such as Moonbird, LUNAv2, Elizabeth, TRUMP, etc., which usually go online quickly and rug with the money in a flash.

II.
2022 Crypto Crime, Financial Risk and Regulation

Contributors:
HELP University：Lee Kheng Joo

Legal DAO：
Master Li, Virgil Ho, Carrie Gan, Ryan Huang, Will Liao, Louise Zhang, Joanna Jing

1. Global Crypto Crime Statistics and Cases

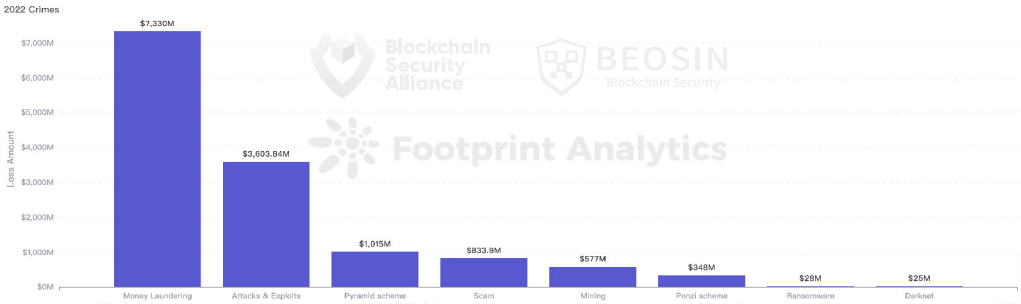
(1) 2022 Global Crypto Crime Statistics

According to statistics from Beosin KYT – the cyrpto AML compliance and analytics platform, global crypto crimes amounted to $13.76 billion for the year 2022 (financial crimes are excluded), with money laundering accounting for $7.33 billion, attacks/exploits $3.6 billion, pyramid schemes $1 billion and scams $830 million.

The money laundering amount accounts for 53% of total crypto crimes, some of which involves cross-border money laundering, placing a high demand on the ability of global regulatory systems to collaborate across borders. Attacks and exploits (see Section 1 for more details) increased significantly in 2022, with very few of these cases seeing hackers being arrested or asset being recovered, leaving an urgent need for global regulators, exchanges, users, projects, and security companies to work together to fill the regulatory gaps.

Pyramid schemes, which accounted for $1 billion in 2022, often involves a large number of users and poses a danger that should not be underestimated.

The global figures for the crypto scams category totaled $830 million, with 51% of that amount coming from rug pulls.



(Remark: Financial risk events are not counted)

(2) Cases of scams

In November 2022, the United States Attorney's Office for the Southern District of New York announced that James Zhong had pleaded guilty to a telecom fraud. James Zhong was accused of illegally obtaining bitcoins from the Silk Road darknet in 2012. In November 2021, law enforcement seized 50,676 bitcoins hidden in equipment at the defendant's home, then worth over US $3.36 billion. The seizure was then the largest cryptocurrency seizure in the history of the US Department of Justice and the second largest financial seizure ever undertaken by the US Department of Justice.

In November 2022, police in London, England, uncovered one of the "largest fraudulent operations in the UK's history," with more than 100 people arrested and approximately £3.2 million ($3.9 million) involved. The criminals used a fraudulent website called iSpoof to impersonate officials from well-known banks such as Barclays, Santander, and HSBC and paid for services using Bitcoin, and police narrowed down the suspects by tracking the Bitcoin records used to pay for the services.

In August 2022, Faruk Fatih Ozer, founder of the Turkish cryptocurrency exchange Thodex, was arrested in the Albanian city of Elbasan. He was wanted by Turkish authorities for more than a year on charges of running a fraudulent cryptocurrency scheme, and in 2021, he received a "Red Notice" from Interpol for his alleged involvement in the country's largest-ever fraud, worth around $2 billion.

In February 2022, the US Department of Justice announcement stated that BitConnect founder Satish Kumbhani was accused of orchestrating a worldwide Ponzi scheme involving approximately $2.4 billion. The announcement stated that BitConnect was an allegedly fraudulent cryptocurrency investment platform that had a market cap of $3.4 billion.

(3) Cases of money laundering

In November 2022, the US Department of Justice announced the arrest of two Estonian citizens charged with 18 counts for their alleged involvement in $575 million in cryptocurrency fraud and money laundering. According to court documents, they defrauded over 100 thousand victims by inducing them to sign fraudulent equipment leasing contracts. The case is currently being investigated by the US Federal Bureau of Investigation.

In September 2022, Dutch police announced the arrest of a male suspect in cryptocurrency money laundering through Bitcoin and Monero coins, involving 10 million+ of euros. The suspect was identified by police after tracing bitcoin transactions and the funds involved were stolen from open source wallets that were updated through the use of malware.

In February 2022, the US Department of Justice announced that two individuals had been arrested on suspicion of cryptocurrency money laundering offences. The cryptocurrencies involved are suspected to be those stolen from the 2016 hack of the crypto exchange Bitfinex, and the cryptocurrencies involved were worth approximately $4.5 billion at the time of the announcement. At the time of the announcement, law enforcement had seized over $3.6 billion worth of cryptocurrency in connection with the hack.

2. Regulatory Responses Arising From Financial Risks

In 2022, the crypto market has seen a series of black swan events represented by Three Arrows Capital, Terra Luna and FTX. For this crypto market, which has grown significantly in the past decade, various jurisdictions around the world have shown a lack of regulations, or even fallen into a regulatory void. With this background, the global Web3 highlands are accelerating the development of regulatory frameworks, and by 2023 the global crypto market will have moved from the "Wild West" to the "Age of Law", with global regulators expected to reach initial cooperation on the crypto market.

(1) Tornado Cash

1. Overview

On August 8, 2022, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) announced that it had placed the Tornado Cash on the Specially Designated Nationals and Blocked Persons List (SDN List). Subsequently, Alexey Pertsev, the developer of Tornado Cash, was arrested in the Netherlands on suspicion of involvement in the development of Tornado Cash, concealing the flow of criminal funds, and facilitating money laundering. OFAC claims that since 2019, more than $7 billion has been used to launder criminal funds using Tornado Cash, and that Tornado Cash has provided materially assistance, sponsorship, or financial and technical support to illegal cyber activities inside and outside the United States that Tornado Cash has been sanctioned by OFAC for acts that may pose a significant threat to the national security, foreign policy, economic health, and financial stability of the United States.

2. Regulatory Responses

The mission of the Office of Foreign Assets Control (OFAC), an agency of the U.S. Department of the Treasury, is to administer and enforce all economic and trade sanctions based on U.S. national security and foreign policy, including financial sector sanctions for all acts of terrorism, transnational drug and narcotics trade, and proliferation of weapons of mass destruction.

Prior to the sanctions on Tornado Cash, the team was also repeatedly contacted by regulators to provide appropriate controls regarding illegal money laundering, but the team stated that it had no control over the decentralized on-chain protocol and argued that the decentralization feature could circumvent regulation (at least FinCEN argued that non-custodial, automatically executed software programs are not 'Money Transmitter' and do not trigger compliance with the U.S. Bank Secrecy Act).

OFAC has since imposed direct sanctions against Tornado Cash, stating in a press release that "Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks. Treasury will continue to aggressively pursue actions against mixers that launder virtual currency for criminals and those who assist them."

(2) FTX / Luna / 3AC

A) FTX

1. Overview

FTX was once the second largest cryptocurrency trading platform in the world. On Nov. 11, FTX said in an announcement via its official social media accounts that FTX Trading, FTX USA, Alameda Research and about 130 other affiliates began voluntary bankruptcy proceedings. In bankruptcy documents obtained by U.S. media, FTX said it has more than 100,000 creditors and that the company currently has between $10 billion and $50 billion in assets and between $10 billion and $50 billion in liabilities. As of now, the US White House, SEC (Securities and Exchange Commission), Bahamas police and many other regulators are investigating the matter, and top international investment institutions such as Sequoia, Temasek, Ontario Pension Fund and SoftBank are among the victims. The debt crisis, which is bound to go down in the history books of the cryptocurrency sector and will even leave a mark in financial history, is still spreading – several crypto platforms have announced that they are in liquidity crisis due to FTX.

2. Regulatory Responses

After FTX declared bankruptcy, Japan's Financial Services Agency requested FTX's branch in Japan to cease operations immediately. The SEC disclosed that it had filed charges against SBF on December 13, 2022 for violating the antifraud provisions of the securities laws and is seeking an order prohibiting SBF from participating in any offering, sale, or purchase of securities using a non–personal account, as well as a ban on acting as an officer, forfeiture of proceeds of violations, and civil damages. The Southern District of New York Attorney's Office and the CFTC have also filed charges against SBF, who was arrested in the Bahamas on December 13, 2022. The Bahamian government is also conducting civil and criminal investigations into SBF and FTX.

B) Terra Luna

1. Overview

In May this year, TerraUSD (UST), an algorithmic stable coin, and Luna, a token, plummeted and crashed the cryptocurrency, with the price of Luna dropping from nearly $90 to less than $0.00015, which was called a "value destruction machine" and many investors suffered great losses. Luna is Terra's platform token, designed to absorb the volatility of UST. In May, the UST suddenly depegged from its anchor currency, the US dollar, and as the price of the UST fell, holders exchanged it for Luna and sold off Luna, sending the two coins into a death spiral, resulting in the collapse of Luna and a sharp drop in its total market value.

2. Regulatory Responses

Luna victims filed a lawsuit against Terra CEO Do Kwon in South Korea, accusing him of fraud and causing investors to suffer huge losses by failing to truthfully inform them of the risks of cryptocurrencies, and the Korean Joint Financial and Securities Crimes Investigation Unit launched an investigation into Terra. Do Kwon was convicted of violating South Korea's Capital Markets Act and was granted arrest by a South Korean court. On September 14, 2022, a South Korean court issued an arrest warrant for for the lead developer of Luna.

C) Three Arrows Capital

1. Overview

Three Arrows Capital used to be one of the largest hedge funds in the cryptocurrency market, and as recently as March this year, its assets under management reached $10 billion, with a portfolio that included tokens such as Avalanche, Solana, Polkadot and Terra. As the plunge of stablecoin TerraUSD and its sister token Luna brought down the entire cryptocurrency market in May, coupled with a margin call on the loan, Three Arrows Capital was rumored to be in bankruptcy and liquidation in late June.

2. Regulatory Responses

On June 22, 2022, the BVI Court ordered the liquidation of Three Arrows Capital, and on July 1, 2022, Three Arrows Capital filed Chapter 11 proceedings in the United States Bankruptcy Court for the Southern District of New York with respect to its assets in the United States, and the Court agreed to grant Chapter 11 protection to its assets in the United States.

3. Regulatory Compliance in Different Countries & Regions

3.1 United States

As a global leader in the crypto industry, the U.S. has not yet formed a unified regulatory structure for the crypto market as of the end of 2022, with a "multi-regulatory" dynamic. A unified approach to the crypto market is emerging in the U.S.,which is to accelerate regulatory innovation and not miss any revolutionary opportunities. At the congressional legislative level, several crypto bills have been introduced in Congress, most of which are still in the early stages of committee consideration. On the administrative enforcement front, regulators are also exploring regulatory paths in the form of "Regulation by Enforcement" (the U.S. is a case law country, and case law is the primary source of law in the U.S.).

The following is a selection of some of the major events that occurred in the U.S. in 2022 with respect to crypto market regulation to reflect the changing regulatory landscape.

On March 10, 2022, the U.S. White House released an executive order titled "Ensuring Responsible Development of Digital Assets" which recognizes the tremendous growth of the crypto market and formally states its desire to ensure that the U.S. continues to lead the way as an "innovation zone" for the crypto industry. The Executive Order makes clear for the first time that this is an "official all-hands-on-deck" mandate, and coordinates the implementation of the Order across multiple departments.

On April 28, 2022, U.S. Representative Glenn Thompson introduced proposed legislation called the Digital Commodity Exchange Act of 2022 (DCEA), which seeks to delegate most of its authority to the CFTC and expand its regulatory authority to the spot market for digital assets based on the CFTC's existing framework. In addition, the proposed legislation imposes more stringent requirements on stablecoin issuers.

On June 7, 2022, Republican U.S. Senator Cynthia M. Lummis introduced a legislative proposal called the Responsible Financial Innovation Act, which would combine with existing law to create a more comprehensive regulatory framework for digital assets, attempting to "pragmatically" respond to current digital asset. The Act seeks to strike a balance between consumer protection, regulatory transparency, the promotion of financial innovation and market flexibility.

On August 3, 2022, Democratic Senator Debbie Stabenow introduced proposed legislation called the Digital Commodities Consumer Protection Act of 2022 (DCCPA), to give the CFTC greater regulatory authority over cryptocurrency markets and exchanges, which was strongly supported by the FTX's SBF.

On August 8, 2022, OFAC announced sanctions against the crypto mixer Tornado Cash, saying it helped launder more than $7 billion in criminal funds and that these actions could pose a significant threat to the national security of the United States. Critics within the crypto industry objected to OFAC's decision to blacklist the code, rather than specific individuals or businesses, in this case.

On September 15, 2022, Ethereum completed its "merge" from POW to POS, with SEC Chairman Gary Gensler commenting that as a result of this change, the whole of Ethereum will become a security and should be regulated by the SEC.

On September 16, 2022, the White House released the "First-Ever Comprehensive Framework for Responsible Development of Digital Assets" to promote multi-sector cooperation, provide clearer direction for the regulation of cryptoassets at the U.S. administrative level, and emphasize U.S. leadership in the global financial system and cryptoassets.

On September 22, 2022, the CFTC took its first enforcement action against Ooki DAO. In addition to charging the organization with operating an illegal commodity futures platform, the CFTC also penalized members of Ooki DAO, and any member who held tokens and voted on DAO proposals could be subject to CFTC penalties for DAO violations.

On October 10, 2022, ahead of a series of G20 meetings, the Global Financial Stability Board (FSB) published a proposed framework for the international regulation of crypto-asset activities. The report contains nine recommendations on regulation, information exchange, governance, and disclosure aimed at driving global regulators to strengthen regulation of crypto markets.

3.2 EU

The EU is relatively friendly to the cryptoasset market, but does not have a clear regulatory framework. Cryptoassets are defined as Qualified Financial Instruments (QFI's) and EU law does not prohibit financial firms from holding, trading and providing services related to cryptoassets. Subjects trading in QFI's are regulated at the individual EU member state level and can simply rely on existing QFi licenses to offer crypto asset-related products and services within member states, while at the same time having to comply with a wide range of EU crypto asset rules and regulations, including AML/CTF, CRD/CRR, EMD2, MiFID II, PSD2, compensation, margin, deposit and sanction obligations, etc.

On October 10, 2022, the European Parliament preliminarily adopted the proposed legislation "The Markets in Crypto-assets Regulation (MiCA)", which paved the way for the subsequent adoption of the bill in the plenary session of the EU Parliament, which is expected to enter into force in early 2024. Once formally approved, the MiCA will establish uniform definitions (at the EU level) of key terms for all activities related to the crypto-assets market in order to regulate it. In general, the MiCA will mainly regulate (i) crypto-assets of all types and (ii) crypto-asset services and service-providers of all types.

On October 10, 2022, the European Parliament initially adopted proposed legislation for the Transfer of Funds Regulation (TFR), an anti-money laundering law that would require all crypto-asset transactions to be traceable and require crypto-asset service providers to continuously monitor any third-party transfers to their customers, but not non-custodial wallets for P2P transactions. The bill is pending final passage.

On November 10, 2022, the European Parliament adopted the Digital Operational Resilience Act (DORA), a cybersecurity legislation for digital finance and crypto-asset service providers that aims to harmonize risk management requirements and processes for reporting cybersecurity incidents to enhance the resilience of their digital operations and prevent and mitigate cyber threats. Financial institutions will be required to monitor and report security incidents, and technology service providers will be subject to oversight by European regulators.

On December 15, 2022, the European Securities and Markets Authority (ESMA) issued a guidance document for the DLT pilot project that allows market participants to trade and settle using stablecoins prior to the implementation of a legal framework for cryptocurrencies. Crypto exchanges and crypto service providers can apply for access to the regulatory sandbox in accordance with the guidance document, thus exempting them from some of the financial regulatory obligations that traditional financial institutions must comply with. The project will be launched in March 2023.

3.3 Hong Kong SAR & Singapore

In 2022, as a leader in cryptocurrency regulation in Asia, Singapore continues to be active in this area, especially in the wake of a series of financial events that have led to regulatory changes and adjustments. Hong Kong, on the other hand, is poised to unleash its cryptocurrency and Web 3 world friendliness through a series of regulatory and legislative changes in 2022, signaling its determination to keep up with today's new economic trends. This section presents a selection of key events in cryptocurrency regulation in Hong Kong SAR and Singapore in 2022 to reflect the changing regulatory dynamics.

Hong Kong SAR

On January 12, 2022, the Hong Kong Monetary Authority (HKMA) issued a discussion paper on crypto-assets and stable-coins, "Discussion Paper on Crypto-assets and Stablecoins", inviting the industry and the public to comment on the relevant regulatory model, firing the first shot in the crypto regulatory arena in 2022 from the Hong Kong side.

On January 28, 2022, the Securities and Futures Commission (SFC) and the HKMA issued a Joint Circular on Intermediaries' Virtual Asset-Related Activities, which sets out the latest guidance on intermediaries' distribution of virtual asset-related products or provision of virtual asset trading or advice services to clients on virtual assets. On the same day, the HKMA also issued a separate Circular on Business Connection between Authorized Institutions and Virtual Assets and Virtual Assets Service Providers. The circular states that it is not the HKMA's intention to prohibit AIs from taking financial risks in relation to virtual assets, for example, by investing in virtual assets, lending against virtual assets as collateral, or allowing customers to use credit cards or other payment services to access virtual assets. This is provided that AIs have adequate risk controls in place and that such activities are adequately supervised by senior management. In addition, the Office of the Superintendent of Insurance has issued a "Circular Letter on Supervisory Approaches to Virtual Assets and Virtual Asset Service Providers" to authorized insurers, reminding them of their obligations under the Enterprise Risk Management Guidance (GL21) when assessing and addressing risks associated with virtual asset-related activities.

On July 6, 2022, the draft amendments to the Anti-Money Laundering and Terrorist Financing Ordinance (Cap. 615) were read for the first time in the Hong Kong Legislative Council, and on July 11, the amendments were formally tabled in the Legislative Council. One of the purposes of the draft amendments is to establish a licensing regime for virtual asset service providers ("VASP"), which includes provisions to combat money laundering and terrorist financing, and to protect investors. Prior to this, Hong Kong did not have a regulatory regime specifically for virtual asset service providers, and generally applied the Securities and Futures Ordinance, which applies to ordinary securities, thus creating a certain lack of clarity and confusion for virtual asset exchanges to apply for licenses, and not many organizations obtained the relevant licenses. Hashkey and Huobi were among the earlier organizations to obtain the relevant licenses in Hong Kong. In April, 2022, HashKey obtained the Hong Kong Securities and Futures Commission Class 1 (securities trading) and Class 7 (automated trading services) licenses, and again obtained the Class 9 (asset management) license in September this year, thus obtaining a full type of portfolio license for virtual assets. In July 2020, Huobi was granted Class 4 (advising on securities) license and Class 9 (asset management) license. On July 14 this year, the Hong Kong Securities and Futures Commission has officially accepted Huobi's Class 1 and Class 7 license applications, which have not yet been approved.

On October 31, 2022, the first day of Hong Kong Fintech Week, the Financial Secretary of Hongkong released the much-anticipated "Policy Statement on Virtual Asset Development", releasing an open and friendly attitude towards virtual assets. The Hong Kong Securities and Futures Commission, on the same day, issued a Circular on Virtual Asset Futures Exchange Traded Funds, indicating that it would authorize the first public offering of virtual asset index funds (ETFs) in Hong Kong under Sections 104 and 105 of the Securities and Futures Ordinance.

On December 8, 2022, the Legislative Council of Hong Kong formally passed the Anti-Money Laundering and Counter-Terrorist Financing (Amendment) Bill 2022 to strengthen Hong Kong's anti-money laundering and terrorist financing regime and to establish a comprehensive and balanced regulatory framework for virtual asset activities to protect investors. A person who engages in the business of operating a virtual asset exchange must apply for a license from the Securities and Futures Commission (SFC).

On December 14, 2022, the SFC issued a Statement on Statement on virtual asset arrangements claiming to offer returns to investors, stating that while there have been a number of recent incidents in the virtual asset industry, virtual asset platforms offering virtual asset deposits, savings, income or pledge services (virtual asset arrangements) to investors in Hong Kong continue to be prevalent.

On December 16, 2022, the Virtual Asset ETF was officially listed and traded on the Hong Kong Stock Exchange, which is the first Virtual Asset ETF in the Asian market and marks a key step in the development of virtual assets in Hong Kong.

Singapore

On January 17, 2022, the Monetary Authority of Singapore (MAS) issued Guidelines on Provision of Digital Payment Token Services, which clearly warned that cryptocurrencies are high-risk and unsuitable for investment by the general public; limited operators to publicly marketing them on their respective websites, mobile apps or official social media accounts; and issued a National Financial Education case study to explain the high risks of cryptocurrency trading.

On February 18, 2022, Tharman Shanmugaratnam, Senior Minister of the Monetary Authority of Singapore (MAS), stated that there are no plans to regulate NFT and that the regulator has taken a "technology-neutral" stance on NFT and that it is not the purview of MAS to regulate everything that people choose to invest in. However, MAS' position on NFT may change, saying that if NFT represents the right to invest in a portfolio of listed stocks, it will be subject to the same prospectus, licensing and business conduct requirements as other collective investment schemes.

On March 11, 2022, Singapore's Finance Minister Lawrence Wong told Parliament that Singapore's current income tax rules would apply to NFT transactions as well as to individuals trading NFTs, and that the income tax treatment would be determined by the nature and use of the NFT. In addition, Wong noted that since Singapore does not have a capital gains tax regime, individuals are not taxed on capital gains from NFT transactions.

The Singapore Parliament passed the Financial Services and Markets Bill 2022 on April 5, 2022, which strengthens anti-money laundering and anti-terrorist financing related to cryptocurrencies. Two major highlights are worth noting: (1) Expansion of regulated conduct: the definition of DPT services is aligned with the Financial Action Task Force (FATF) standards, including direct or indirect trading, exchange, transfer, custody of cryptocurrencies, or providing related investment advice; (2) Increase of regulated institutions: covering cryptocurrency operators established in Singapore (but providing services outside Singapore), so as not to damage the reputation of Singapore's financial market, so as not to damage the reputation of Singapore's financial markets.

The cryptocurrency licensing regime in Singapore needs to be stringent and should not market cryptocurrencies to the public, said Ravi Menon, Managing Director of the Monetary Authority of Singapore, in a speech to the crowd at the Crypto and Digital Asset Summit held by the Financial Times on April 27, 2022. The MAS wants to provide clarity to the cryptocurrency industry and needs to ensure that stable coins are backed by liquid assets and does not believe that cryptocurrencies pose a significant financial system risk.

On June 8, 2022, Singapore's digital securities platform ADDX announced it was the first financial firm in the country to recognize cryptocurrencies when valuing the assets of high-net-worth clients. ADDX said it will only recognize cryptocurrencies with a high market value and will use a discount rate when valuing these assets. ADDX CEO Oi-Yee Choo said, "In future, we are likely to enable customers to fund their investment wallets with cryptocurrencies and to convert their assets between fiat currencies and crypto."

On July 19, 2022, Ravi Menon, Managing Director of the Monetary Authority of Singapore (MAS), said that the focus of crypto regulation in Singapore and most major jurisdictions has so far been on curbing money laundering and terrorist financing risks, although this trend is shifting and MAS plans to consult on proposed measures in the coming months. In addition, MAS will host a special workshop next month to share strategies aimed at developing Singapore into a digital asset hub. In addition, Ravi Menon clarified that some so-called "Singapore crypto companies" actually have little to do with crypto-related regulation in Singapore, such as TerraForm Labs and Luna Foundation Guard, which are not licensed or regulated by MAS and have not applied for any licenses or sought exemptions from holding any licenses; Three Arrows Capital is not regulated under the Payment Services Act; and Vauld is not currently licensed by MAS and has not sought exemptions under the Payment Services Act.

On July 20, 2022, the Blockchain Association of Singapore (BAS) and Daimler Southeast Asia have entered into a strategic partnership through the signing of a Memorandum of Understanding (MOU) to launch Acentrik, Daimler Southeast Asia's strategic initiative to unlock the potential of data in the enterprise and enable token-based monetization in B2B environments. Acentrik and BAS will collaborate on related blockchain initiatives to work with existing and potential enterprises within the BAS community, and the two companies will also work to drive enterprise adoption of blockchain-based data marketplaces at a cross-industry level to help businesses and industries accomplish growth and transformation.

On August 29, 2022, the Monetary Authority of Singapore (MAS) said it is considering the introduction of cryptocurrency measures that may include limiting consumer leverage to reduce the harm to consumers from cryptocurrency transactions and will also propose a regulatory approach for stablecoins. The MAS will conduct a public consultation on the new measures by October. Earlier in August, Singapore's Senior Minister Tharman Shanmugaratnam said in response to the UST and LUNA crashes that it was actively reviewing the approach to regulating stablecoins and assessing the merits of a regulatory regime tailored to the specific characteristics and risks of stablecoins, such as regulatory reserve requirements and stablecoin pegs, and would seek public comment in the coming months.

On October 6, 2022, in response to a parliamentary question, Tharman Shanmugaratnam, Senior Minister and Minister in Charge of the Monetary Authority of Singapore, stated that not all activities related to digital payment tokens (DPT) are regulated and that companies providing services involving the purchase, sale or facilitation of DPT exchanges will be regulated under Singapore's Payment Services Act 2019 (PS Act).

On October 18, 2022, INTERPOL indicated it would form a dedicated team in Singapore to help countries fight crimes involving crypto-assets. INTERPOL Secretary General Jürgen Stock said that cryptocurrencies such as Bitcoin and Ether pose a challenge to law enforcement agencies in the absence of a legal framework.

In two consultation papers released on Oct. 26, 2022, the Monetary Authority of Singapore (MAS) proposed restricting retail investors from borrowing money or using credit cards to buy cryptocurrencies and from lending their digital tokens in search of proceeds. The authority also wants cryptocurrency exchanges to quiz potential cryptocurrency buyers to see if they understand the risks of what it calls a "highly volatile" asset class.

November 2, 2022 saw a small spike in cryptocurrency regulation in Singapore.

1. First, USDC stablecoin issuer Circle announced that it has received regulatory approval in principle in Singapore, having been granted a Major Payments Institution License by the Monetary Authority of Singapore (MAS), thus enabling Circle to offer digital payment token products, cross-border and domestic remittance services in Singapore.

1. First, USDC stablecoin issuer Circle announced that it has received regulatory approval in principle in Singapore, having been granted a Major Payments Institution License by the Monetary Authority of Singapore (MAS), thus enabling Circle to offer digital payment token products, cross-border and domestic remittance services in Singapore.

2. Secondly, USDP issuer Paxos also announced that it has been granted this license by MAS, enabling it to offer digital assets and blockchain products and services to companies in Singapore.

3. In addition, MAS announced the launch of its Digital Asset Pilot and Decentralized Finance (DeFi) service, and the first industry pilot under its Project Guardian to explore potential Decentralized Finance (DeFi) applications in the wholesale financing market has completed its first live transaction. In the meantime, it has launched additional industry pilots to test the application of asset tokenization and DeFi in broader use cases in the financial sector. In terms of details.

a. Under the first industry pilot, DBS Bank, JPMorgan Chase and SBI Digital Asset Holdings traded foreign exchange and government bonds against a liquidity pool that included tokenized assets.

b. Successful placements involving tokenized Japanese yen and Singapore dollar deposits.

c. Real-time transactions executed under the first pilot demonstrated that DeFi enables instant trading, clearing and settlement by participants in cross-currency transactions of tokenized assets without the need for financial intermediaries.

d. Forum Orwell, in partnership with DBS Bank, JPMorgan Chase and SBI Digital Asset Holdings, has published a white paper summarizing the broad lessons learned from the first pilot, including the benefits of digital asset interoperability and transaction efficiency that institutional DeFi protocols can introduce into the financial markets.

4. In addition, MAS is launching two new industry pilots in trade finance and wealth management.

On November 21, 2022, the Monetary Authority of Singapore (MAS) stated in a post on its website that the reason for MAS' previous inclusion of Binance on the Investor Alert List (IAL) and not FTX on that list is that while neither is licensed, there is a clear solicitation of Singaporean users by Binance, while FTX is not. In fact, Binance has been able to denominate in Singapore dollars and accept payment methods specific to Singapore, such as PayNow and PayLah. MAS is unlikely to list all offshore cryptocurrency exchanges on the IAL, but will only warn subjects that have committed possible violations in Singapore. Furthermore, MAS has stated that even if cryptocurrency exchanges are licensed in Singapore, they will only be regulated in areas such as anti-money laundering, and will not protect investors.

3.4 Japan & South Korea

In Japan, no comprehensive regulatory policy has been explicitly introduced for blockchain-based digital assets. The legal status of crypto assets under current Japanese law is determined by their function and use, but Japan has been at the forefront of crypto asset regulation.

In 2016, Japan revised the Payment Services Act and the Money Services Act, which were formally established in 2017, to clarify the legal status of cryptocurrencies.

On the one hand, cryptocurrencies are considered as "crypto assets" in the Payment Services Act. Operators who engage in the business of buying, selling, or administering crypto assets (and intermediating such activities) or managing crypto assets for the benefit of others must register as a cryptocurrency asset transaction service.

On the other hand, the Financial Services Agency, Japan's financial regulator, regulates cryptocurrency exchanges through the Financial Instruments and Exchange Act (FIEA), and investment interests in partnerships that are transferable through the blockchain, etc., are considered marketable securities (i.e., general partnership securities that are transferred by non-electronic means). Under the FIEA regulations, the business of providing or acting as an intermediary in providing derivatives related to crypto assets is a Class 1 financial instrument business. The related business constitutes an investment advisory business or an investment management business and is required to register accordingly under the FIEA.

As for stablecoins, the Japanese government believes that depending on whether such stablecoins are convertible in fiat currency, stablecoins may be classified as crypto assets or as a means of payment in remittances. In addition, since NFT is not currently considered to function as a means of payment, no agreement has been made under the current regulatory framework, but the Financial Services Agency, Japan's financial regulator, has added the matter of establishing a regulatory framework for NFT to its agenda.

South Korea is also not to be overlooked as an important digital asset trading region in Asia. Unlike other regions, South Korea has acted more actively in terms of crypto regulation.

As early as late 2016, South Korea established a digital currency working group, and in 2017, a revised version of the Korea Foreign Exchange Trading Act allowed fintech companies to register with the Financial Supervisory Service (FSS) to "provide international currency transfer services for small amounts of money," including bitcoin. On January 30, 2018, South Korea began implementing a real-name system for virtual currency transactions.

In 2020, the full South Korean National Assembly formally passed the amendment to the Special Financial Information Act, which defines crypto asset-related businesses as Virtual Asset Service Providers (VASPs). Digital asset operators must comply with operator operations, such as reporting to the Financial Information Analysis Unit (FIU) of the Korea Financial Commission, anti-money laundering obligations (customer confirmation and suspicious transaction reports, etc.) and additional obligations. Specifically, failure to report business operations will be punishable by up to five years in prison and a fine of up to KRW 50 million. This means that the government will directly regulate the cryptocurrency market within the scope of the law.

And in 2022, South Korea made further amendments to the Special Financial Information Act, stating that cryptocurrency exchanges must develop and implement business guidelines to prevent operators and executives from trading virtual currencies on the exchanges where they work. Insider trading is only allowed if cryptocurrencies are converted into Korean won for tax purposes.

Nonetheless, Japan and South Korea are still in the process of trial and adjustment in the regulation of crypto assets, and the relevant policies will evolve gradually as the crypto sector develops.

3.5 Malaysia

Labuan International Business and Financial Centre (IBFC) is a special economic zone of the Malaysian government based on the island of Labuan off the Borneo coast. It was established in 1990 as part of the government's effort to boost the financial industry of Malaysia at the international level.

Labuan Financial Services Authority (Labuan FSA) was established on 15 February 1996 under the Labuan Financial Services Authority Act 1996. Labuan FSA is the statutory body responsible for the development and administration of the Labuan International Business and Financial Centre (Labuan IBFC).

Labuan FSA licenses and regulates licensed entities operating within Labuan IBFC and to ensure all such entities remain in compliance with the Labuan laws and regulations and adhere to the international standards, that are adopted by the jurisdiction.

Labuan IBFC support a fit-for-digital business structures to facilitate various digital financial-related services (DFS) in the Centre. These include digital-banking, fintech, payment services, insurtech business to digital intermediaries such as Robo-advisors, digital asset exchanges, crypto trading platforms, blockchain tokens as well as e-payment systems. Labuan entities are required to obtain Labuan FSA's prior approval before undertaking proposed DFS-related activities.
Currently the FSA have issued about 800 licences of which about 85 are Digital Financial Services (DFS). Was reported that there are 5 digital trading platform licence issued (will verify)

To facilitate virtual and non-face-to-face contact of DFS businesses, there will be subsequent regulations and guidelines on eSignature and eKYC Regulatory emphasis will be on the compliance to the AML (Anti Money Laundering)/CFT (Counter Financing for Terrorism) and market conduct requirements. This is critical to ensure that all DFS activities in the Centre is not used to front any money laundering or terrorism financing schemes; whilst promoting professional and transparent services in dealings with clients.

Labuan is considered a tax haven due to its favourable tax structures for non-residents and has become one of the preferred jurisdictions in Asia for offshore company formation.

The Labuan IBFC has a tax efficient regime, the rate of tax imposed is 3% of audited net profits for trading activity and zero percent for non-trading activity, provided that the Labuan entities are in compliance with the tax substantial activity requirements. However, Labuan entities are exempted from withholding tax on those specified payments made to non-residents.

Licence holders are required to submit regular reports on AML/CFT (counter financing for terrorism), robustness of systems and IT, business continuity assessment, risk management and marketing activities.

The Labuan IBFC is a member and signatory of the international agencies and best practices of the following organisations. APG https://apgml.org/ (Asia Pacific Group on Money Laundering), International Organisation of Securities Commission https://www.iosco.org/, The Financial Action Task Force https://www.fatf-gafi.org/ International Association of Insurance Supervisors (IAIS) https://www.iaisweb.org/

Islamic Financial Services Board https://www.ifsb.org/ International Islamic Financial Market https://www.iifm.net/

3.6 The United Arab Emirates-Dubai

On February 28, 2022, Dubai enacted "Decree No. (4) – Regulation of Virtual Assets in the Emirate of Dubai". Dubai establishes the Dubai Virtual Assets Regulatory Authority (VARA) and gives VARA regulatory powers in all areas except the Dubai International Financial Centre (DIFC), which remains under the control of the Dubai Financial Services Authority (DFSA). Through this decree, Dubai hopes to establish a basic regulatory structure for virtual assets that will protect investors and the growth of the industry. Under this Decree, any person or company wishing to conduct activities regulated by this Decree in the Emirate of Dubai will need to register an entity in the Emirate of Dubai and obtain approval from the relevant Business Regulatory Authority and will need to obtain a VARA wholesale license.

On March 8, 2022, the DFSA issued a consultation paper on the regulation of crypto-tokens (CP143), in which the different types of digital currencies are more specifically defined and a set of related regulatory policies are developed. DFSA hopes to optimize this regulation through feedback from the market and relevant institutions. Note that this regulation is only applicable to the Dubai International Financial Centre region.

On August 18, 2022, VARA adopted a 'Minimum Viable Product' testing phase for virtual assets in Dubai, during which UAE approved Virtual Asset Service Providers (VASPs) to conduct relevant activities in the Dubai region after obtaining a Minimum Viable Product License (MVP). VARA will move to the next regulatory phase when a more complete regulatory framework for the market is ready, and VARA recommends that VASPs apply for a Full Market Product (FMP) license at that time. In addition to this, VARA has issued two Executive Orders that govern marketing practices and penalties for non-compliance, respectively.

On October 17, 2022, DFSA issued its Final Response to CP143 – Regulation of Crypto Tokens, which provides a final decision on the matters explored in draft CP143. Within this regulatory bill, the DFSA divides digital currencies into roughly three categories, governed cryptocurrencies, ungoverned tokens, and outright banned tokens. Jurisdictional cryptocurrencies include three types, 1. currencies that can be used for payment or as a medium of exchange, 2. currencies that can confer the ability to be used in another currency clause 1, and 3. cryptocurrencies that are anchored to a fiat currency. Cryptocurrencies that are not subject to jurisdiction include three types, 1. NFT, 2. functional currencies, and 3. central government digital currencies. But all issuers of NFT and functional currencies still need to register with DFSA as a specified non-financial institution (DNFBP) unless the amount involved is less than $15,000. And all tokens are required and subject to the UAE and Dubai Financial Centre anti-money laundering regulations. The last category of digital currencies are those completely banned in the Dubai Financial Centre, including algorithmic stablecoins and anonymous coins. Any person wishing to participate in the first category of cryptocurrency related transactions, organization, management, consulting, services or related activities will need to be licensed by the DFSA and will be limited to DFSA approved currencies (as of December 16, 2022, the DFSA has only approved BTC, ETH and LTC), which means that currently digital currency companies in the Dubai International Financial Centre can only perform financial services related to these three digital currencies.

On November 1, 2022, Consultation Paper 143 — Regulation of Crypto Tokens (CP143) came into force and the Dubai Financial Centre's digital currency regulatory regime entered its second phase since 2021. DFSA hopes to find a balance between supporting innovation and fighting crime through its regulatory policy. DFSA recognized three currencies, BTC, ETH and LTC, within the same day.

4. 2023 Global Regulatory and Policy Outlook

In 2022, crypto 'bombshells' exploded frequently, accompanied by a dramatic market downturn that caused severe turmoil in the industry. 2023 will certainly see a response from global regulators. A number of regulatory trends are already emerging in 2022. In our view, one of the overarching themes of global crypto regulatory developments in 2023 is likely to be the "systematisation of the regulatory framework". A large number of jurisdictions with rapidly growing crypto industries (e.g. the US, UK, Canada, etc.) have not yet developed a systematic regulatory framework. In these jurisdictions, there have been a large number of regulations issued by various regulatory or enforcement bodies, but the fragmentation has left many of the underlying legal concepts poorly answered and has made practice difficult. The good news is that we are seeing a clear trend towards 'systematisation' in 2022. As we mentioned earlier in this report, the release of the US White House's "First-Ever Comprehensive Framework for Responsible Development of Digital Assets", the adoption of the EU Parliament's MiCA proposal, and the reference to a "comprehensive regulatory framework" in the Hong Kong Virtual Assets Manifesto, all signal this trend. We hope to see more complete regulatory frameworks coming to fruition by 2023.

The increased regulation of centralised exchanges is self-evident. Crypto-centric finance is already operating closer to traditional financial institutions, but without much regulatory or investor protection obligations, and the outbreaks in 2022 have already created an urgency for regulators, who will have significantly more responsibility for centralised exchanges and custodians in 2023. I expect many of the tools of traditional financial regulation to be "replicated" in the crypto space, such as strong disclosure regimes, reserve systems, etc.

The regulation of stablecoins is likely to be another major topic in 2023. After the tragic Luna incident, regulators will have to pay extra attention to stablecoins issued by non-government entities. We can hopefully see some specific, detailed rules for the regulation of stablecoins being issued in 2023. Another trend that cannot be ignored, of course, is the issuance of stablecoins by central banks of all kinds. I note that at least 100 countries and regions are actively promoting the issuance of central bank stablecoins, and many have already completed their experiments ahead of others. The circulation of central bank stablecoins is bound to bring about significant changes to the way assets flow in the crypto industry, and programmable central bank stablecoins could also completely change the landscape and approach to anti-money laundering and tax regulation. This is certainly something to look forward to.

2022 has been a year of rampant hacking, to the point where the industry has been "overwhelmed". We have seen a number of effective attempts in the crypto industry to prevent hacking or recover stolen assets through technology. The prevalence of hacking places a high demand on the expertise of law enforcement agencies and the efficiency of cross-border collaboration. We hope to see more cases of regulators working with blockchain security companies in 2023 to complete more hacker arrests and asset recoveries, boosting the industry's confidence and sense of security.

—— MasterLi (LegalDAO initiator, Web3 attorney)

References:

[1] https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction
[2] https://www.cftc.gov/PressRoom/PressReleases/8549-22
[3] https://www.justice.gov/opa/pr/empiresx-head-trader-pleads-guilty-global-cryptocurrency-investment-fraud-scheme-amassed
[4] https://www.sec.gov/news/press-release/2022-119
[5] https://www.justice.gov/opa/pr/bitconnect-founder-indicted-global-24-billion-cryptocurrency-scheme
[6] https://www.justice.gov/opa/pr/two-estonian-citizens-arrested-575-million-cryptocurrency-fraud-and-money-laundering-scheme
[7] https://www.politie.nl/nieuws/2022/september/13/03-man-opgepakt-witwassen-cryptovaluta.html
[8] https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency
[9] https://www.cnn.com/2022/10/07/tech/binance-bridge-hack/index.html
[10] https://www.cnn.com/2022/03/29/tech/axie-infinity-ronin-hack/index.html
[11]https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea
[12] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/
[13] https://www.congress.gov/bill/117th-congress/house-bill/7614/all-info
[14] https://www.congress.gov/bill/117th-congress/senate-bill/4356/text
[15] https://www.congress.gov/bill/117th-congress/senate-bill/4760/text?r=3&s=1
[16]https://home.treasury.gov/news/press-releases/jy0916
[17] https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/
[18] https://www.cftc.gov/PressRoom/PressReleases/8590-22
[19] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
[20] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015R0847
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595&qid=1671677635120
[22] https://www.esma.europa.eu/press-news/esma-news/esma-provides-guidance-applicants-under-dlt-pilot-regime
[23] https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=22EC10
[24] https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220128e3.pdf
[25] https://www.ia.org.hk/en/legislative_framework/circulars/reg_matters/files/Cir_dd_28.01.2022.pdf
[26] https://www.8btc.com/article/6785328
[27] https://elaws.e-gov.go.jp/document?lawid=421AC0000000059
[28] https://elaws.e-gov.go.jp/document?lawid=429M60000002007
[29] https://elaws.e-gov.go.jp/document?lawid=340CO0000000321_20220901_504CO0000000268&keyword=%E6%9A%97%E5%8F%B7

III.
Security Guidelines for Web3 Users

Contributor:
Buidler DAO – Jason

The security of Web3 is divided into B-side and C-side, with B-side security events characterized by large amounts and high concentration, but also more diverse means, whereas C-side security events characterized by small amounts (there are also cases of large amount theft of personal wallets) and a high degree of fragmentation. The means of c-side are basically the following.

1. Private Key & Seed Phrase

The private key compromise is the most important type of problem. If it is compromised, it means that you lose all ownership of your wallet and that the other party has complete control over the transfer of any assets in your wallet.

Ways to steal private keys:

1. Private key connected to network

Many users store their private key in plaintext directly on their cloud drive. If your cloud drive password is leaked, or even if a third-party online company leaks data, it could lead to the exposure of your private key. Even if you store it locally on your device, such as in a computer notepad, or in a mobile phone album via screenshots, there is a risk that your private key will be leaked if your device is lost, or if hit by a Trojan horse virus. Account leaks can also lead to the exposure of seed phrases, so plaintext storage in devices with network are at risk of leakage. In addition to this, many users copy and paste their private key when logging in, which also poses a risk of leakage in the process.

2. Fake websites stealing private key

Many users visit trading platforms such as Opensea by searching Google for keywords, but there are a number of fake websites to lure you to click on, and they even rank higher than the real ones in the search results. These websites are fake, from the UI style and functionality to the real ones, and the domain names are very similar. When you open these sites, you are usually asked to log in to a "wallet", which is often accompanied by a fake wallet that is disguised on the site, and your assets are instantly transferred when you log in by typing in the mnemonic in the fake site.

3. Lost of private key

In addition to the theft of assets by hackers, the loss of assets by users who lose their private key should not be underestimated. Many users record their private key in a computer notepad or write it down on a note, which may eventually lead to the loss of the private key when the computer is scrapped or lost, thus making it impossible to retrieve the assets. It is likely that a large number of bot addresses that currently hold assets but have not been traded for a long time are the result of lost private keys, and that these assets will be completely locked up.

Solutions to avoid the above issues:

1. Store private keys correctly

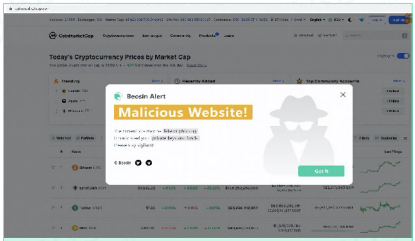
Seed phrases or private keys should not be saved over a network. Do not store it directly in plain text on a cloud drive, do not transmit them through channels such as email, and do not save it in plaintext locally. It is best to save them offline. You can also use multi-signature wallets and smart wallets to save them. As the concept of account abstraction comes to fruition, more and more smart wallets are equipped with capabilities such as social recovery, which is also a big step forward for the safe storage of assets.

2. Copying and pasting seed phrases in sections

Avoid copying and pasting complete seed phrases by copying in sections. If necessary, you can copy in sections. After copying one section, copy something else, then continue to copy another section.

3.Careful when entering private keys or mnemonics

In all cases where you are asked to enter a private key, you can first assume that it is a phishing site and use it in conjunction with security extensions such as Beosin Alert and MetaShield, which will include a blacklist library to assist you in your judgement. The image below shows a fake Coinmarketcap website identified by Beosin Alert.



Add Beosin Alert to your browser:
https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

2. Phishing Websites

Common tricks of phishing websites:

1. Airdrops

If you check your NFT in Opensea, you should find a lot of NFTs you have never seen before in the hide section, and even offers with very high prices, there may be hackers airdropping NFTs to you to lure you into phishing sites. The scheme is actually to lure you to open the airdrop NFT site, and then steal your assets via signature approval, airdrop is only a means to lure you to open the site.

2. Discord DM

It is common in Discord to receive some DMs impersonating the official, telling you to get a certain NFT free mint rights, and then the following will come with a phishing URL. If you click on the button 'mint', pay gas, approve assets, and then you will find your NFT was transferred away.

3. Fake Twitter account

Many upcoming NFTs may face the problem of being registered with fake Twitter accounts, and even these fake accounts have more followers than the real ones. For example, if an NFT project is not yet on sale, but its fake account suddenly announces the sale and puts up a phishing website, then a large number of users who have been looking forward to the project for a long time will be trapped.

4. Offcial Discord/Twitter compromised

This is the most dangerous method of distribution, such as the hacking of the official BAYC Discord server, and other projects where the official Twitter account has been compromised, sending official notices directly to lure people to click on the phishing website.

5. Search engine results

Phishing websites sometimes rank higher than real websites in Google for keywords as the domain names are similar.

Ways to Avoid Phishing:

1. Check the authenticity of sources

Look carefully at the source channel to see if it is official, check that the domain name is correct and think twice before you interact.

2. Be careful with all approvals, transfers and blind signatures

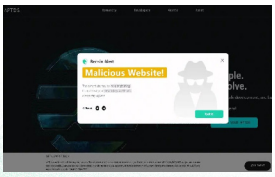
When your wallet asks you to approve and transfer assets, be extremely careful to check whether you really intend to perform such an operation at the moment, and that all blind signatures are done carefully. Check the content and source of the signature to ensure that the operation you are currently being asked to perform is indeed your intention.

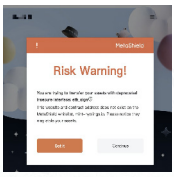
3. Segregation of assets

Always have at least 2 wallets, 1 for small amounts of money for daily transactions, and another for larger amounts of money that you don't use very often, which should only be used to deposit money and avoid transactions as much as possible so that even if you experience a phishing incident, you will have limited assets stolen.

4. Install anti-phishing extension

Install security extensions such as Beosin Alert, MetaShield, etc.





IV.
Beosin's 2023 Blockchain Security Industry Outlook

The year 2022 saw a number of big events in the global crypto market: a significant shrinkage in total crypto marketcap; the collapse of Terra; the bankruptcy of Three Arrows Capital (3AC) and FTX; sanctions against Tornado Cash; the Ethereum merge; and the rapid development of new public blockchains. Amidst the severe shrinkage in marketcap, hackers still stole a record amount of money in 2022. Total losses from attacks reached $3,603.84 million in 2022, an increase of approximately $1.16 billion over 2021. The year 2022 saw a tougher global Web3 security situation than ever before.

Only 8% of the funds from attacks were recovered. It is a fact that the amount of stolen funds flowing into Tornado Cash in the third and fourth quarters decreased significantly compared to the first and second quarters after Tornado Cash was sanctioned in August, but the frequency of attacks and the amount stolen did not decrease in the third and fourth quarters. To truly curb the rampant activities of hackers to any significant degree, multiple efforts are required across the industry, including the following.

1. Rapidly develop and enhance a global regulatory system. The real deterrent is still to resort to legal sanctions for crimes in the crypto space itself. There are already a number of countries where regulatory policies are taking shape, and more countries are expected to systematise their regulatory policies by 2023.

2. Blocking attacks from the source. There are already some successful cases of hacking being blocked by Beosin and other security companies, and as the technology matures, more hacking is expected to be blocked at source in 2023.

3. Stolen funds recovery. Projects, users, security companies, exchanges, and regulators need to work together to locate hackers' on-chain addresses, identifications, entities, etc. As the global regulatory system improves, recovering stolen funds will no longer be a small probability.

4. Strengthen the entire infrastructure. 2023 may see the emergence of new technologies or projects that address the security issues at the infrastructure level. At the same time, the existing blockchain head projects will also optimize their own security system.

5. Security protection from project side. Some projects are developed in a hurry and go live without audit, which is a major cause of attacks. In addition, one weak area in contract security, private key/wallet security, web2 security, or even team operational security can cause a project great damage. For projects, a solution is needed that can take into account all aspects of security. Next year it is expected that more mature projects will find a relatively sophisticated solution.

6. Security for the next narrative. In a bear market, the whole market is waiting for the next narrative of Web3. Once a new trend has just started, it is bound to become a prime target for hackers because of its imperfect maturity and the influx of new users and new projects. Security practitioners across the market must have the ability to learn quickly to meet the emerging challenges of an ever-changing market.

7. Increased security awareness among individual users. The general trend for the next year is to lower the barrier to entry into Web3 for more users, and it is essential to provide them with security knowledge or education.

8. A more convenient and effective governance model. Individual users who suffer asset theft often end up with nothing due to small amounts, fragmented information, low attention and fruitless reporting. Some DAOs have already established initial solutions to such problems, and a better system is expected to emerge next year.

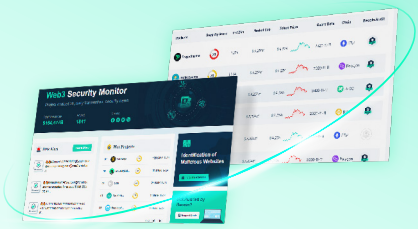
9. A more open and sharing security industry. As mentioned above, all aspects of contract security, private key/wallet security, Web2 security, and team operational security need to be secured, and this requires the joint efforts of the entire security industry. This is also the original intention of Beosin to establish the 'Blockchain Security Alliance'.

Beosin Security Product

Beosin EagleEye

Security monitoring, alerting and blocking

Based on AI technology, combined with on-chain and off-chain real-time data analysis, and open source intelligence, it can timely discover security risks, send alerts and block risk transactions during the operation of Web 3.0 projects. Subscribers will receive real-time warnings for 10 kinds of abnormal risk transactions such as large transfers, flashloans, privilege changes, price drops, etc. It plays a role in hacking, fraud, rug pull and other security issues prevention. Now more than 2,300 Web 3.0 projects have been monitored by Beosin EagleEye.



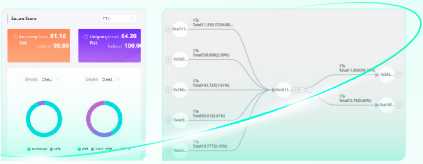
Try Beosin EagleEye: https://eagleeye.beosin.com/

Add Beosin Alert to your browser to detect phishing sites:
https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=en

Beosin KYT

AML and crypto compliance platform

Relying on more than 1 billion address tags and malicious address database, Beosin KYT, the cryptocurrency AML and crypto compliance platform can help VASP (Virtual Asset Service Providers) build KYT (Know Your Transactions) and risk assessment capabilities. The system analyzes massive amounts of on-chain transactions to identify transactions and address types, and then uses the system's massive library of entity addresses and machine learning analytics to assess risky transactions. Beosin KYT are currently serving multiple clients around the world to comply with AML regulations.

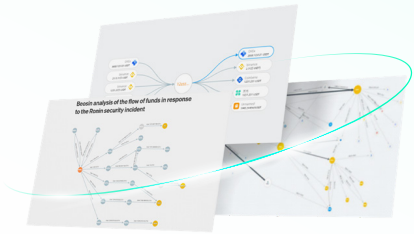


Try Beosin KYT: https://kyt.beosin.com/

Beosin Trace

Cryptocurrency tracing and investigation platform

Beosin-Trace is a cryptocurrency fund tracing platform that combines big data, AI and other technologies. It is a personalized investigation tool for global clients in recovering their lost cryptocurrencies. It has successfully helped clients recover 100+ millions of stolen assets, including funds that flowed into mixers (such as Tornado Cash).

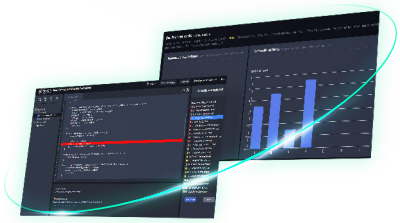


Try Beosin Trace: https://beosin.com/service/tracing

Beosin VaaS

Formal verification platform for smart contracts

Beosin security team uses multiple technologies such as formal verification and fuzzy testing as core technologies to develop VaaS, a highly automated security detection tool for smart contracts, with an accuracy of 97% and can automatically detect hundreds of security vulnerabilities of smart contracts in one-click.



Try Beosin VaaS: https://vaas.beosin.com/

About Blockchain Security Alliance

The Blockchain Security Alliance was initiated by Beosin in joint collaboration with several units from diverse industry backgrounds, including university institutions, blockchain security companies, industry associations, fintech service providers, etc. The first batch of alliance council include Beosin, SUSS NiFT, NUS AIDF, BAS, FOMO Pay, Onchain Custodian, Semisand, Coinhako, ParityBit, and Huawei Cloud. The current members include: Huobi University, Moledao, Least Authority, PlanckX, Coding Girls, Coinlive, Footprint Analytics, Web3Drive, and Digital Treasures Center. The members of the Security Alliance will work and cooperate together to continuously secure the global blockchain ecosystem with their own technical strengths. The Alliance Council also welcomes more people in blockchain-related fields to join and jointly defend the security of the blockchain ecosystem.

Alliance Registration: https://forms.gle/pb3NaUgS3a2Sswnc8

Contact: @kristenbeosin @Web3Donny market@beosin.com

About Beosin

Beosin is a leading global blockchain security company co-founded by several professors from world-renowned universities and there are 40+ PhDs in the team. It has offices in Singapore, UAE, Korea, Japan and other 10+ countries. With the mission of "Securing Blockchain Ecosystem", Beosin provides "All-in-One" blockchain security solution covering Smart Contract Audit, Risk Monitoring & Alert, KYT/AML, and Crypto Tracing. Beosin has already audited more than 2500 smart contracts including famous Web3 projects PancakeSwap, Uniswap, DAI, OKSwap and all of them are monitored by Beosin EagleEye. The KYT AML are serving 100+ institutions including Binance.

About LegalDAO

LegalDAO is a decentralized community that gathers global Web3 legal professionals and enthusiastic participants, dedicated to building a global Web3 legal ecosystem. Through initiating the bottom-up "2023 Crypto Consensus Referendum," establishing a social relationship-based on-chain identity system "De-X," a decentralized self-governance system "De-Reg," and Web3 legal research, education, socialization, and other content, we call on everyone to work together to complete the great practice of establishing Web3 native order.

About Buidler DAO

BuidlerDAO is a crypto community uniting engineers, researchers and operators to produce high-quality content and develop Dapps. We aims to BUIDL an influential and productive leading network for Web3 buidlers and accelerator for projects.

About Footprint Analytics

Footprint Analytics is a tool to uncover and visualize data across the blockchain, including NFT and GameFi data. It currently collects, parses and cleans data from 23 chains and lets users build charts and dashboards without code using a drag-and-drop interface as well as with SQL or Python.

CONTACT US

market@beosin.com
Email

@Beosin
Telegram

@Beosin_com
Official Twitter

@BeosinAlert
Alert Twitter